Before the
Federal Communications Commission
Washington, DC 20554

In the Matter of	
Protecting the Privacy of Customers of Broadband and Other Telecommunications Services	WC Docket No. 16-106
Petition of Public Knowledge et al. for Declaratory Ruling that Section 222 of the Communications Act Prohibits Telecommunications Providers from Selling Non-Aggregate Call Records Without Customers' Consent	WB Docket No. 13-306

REPLY COMMENTS OF NEW AMERICA'S OPEN TECHNOLOGY INSTITUTE

Filed July 6, 2016

TABLE OF CONTENTS

INTRODUCTION AND SUMMARY

In response to the FCC's broadband privacy proposal,[1] BIAS providers[2] and other opponents have mounted a full assault on consumer choice. Their comments are resoundingly anti-consumer. Instead, they prefer to extract more revenues by exploiting data they must collect about their customers' online activities but that rightfully belongs to the customers themselves. Most, if not all, BIAS providers argue that the FCC has insufficient authority to enact these rules. Even if it does have the requisite authority, they argue, the FCC should simply adopt the FTC's approach to privacy—and thereby ignore the particular concerns for communications networks recognized by Congress and encoded in the law. BIAS providers also argue that the proposed rule violates the First Amendment.

All of opponents' arguments fail. The Commission's broadband privacy proposal is reasonable, responsive to the needs of broadband customers and the direction of Congress, and rests on solid statutory footing. In passing Section 222 of the Communications Act, Congress recognized the particular privacy interests of telecommunications customers and created heightened privacy obligations for telecommunications providers.[3] Further, the proposed rule does not violate the First Amendment because of the substantial government interest in protecting consumer privacy and giving consumers options to protect their data, which in

---

[1] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, Notice of Proposed Rulemaking, 31 FCC Rcd 2500 (2016) (Notice).
[2] "BIAS providers" is used interchangeably with "internet service providers," "ISPs," and "broadband providers" in these comments unless otherwise specified.
[3] Even the FTC itself primarily supports the broadband privacy proposal. FTC Comments at 34 ("FTC staff supports the FCC's focus on the core privacy values of transparency, consumer choice, and data security.").

turn promotes unfettered and uninhibited use of the internet. Thus, the FCC should reject in total the ISPs' attempts to water-down the vital consumer protections proposed in the Notice.

I. The Commission has clear statutory authority to enact the proposed rules

Several commenters argue the FCC lacks authority to enact the rule it has proposed. In particular, CTIA and others argue that the FCC has only very limited authority under Sections 222 and 201(b).[4] These arguments are not persuasive, and should be rejected.

A. The Commission has authority under Section 222 to protect "customer PI"

CTIA, Verizon, and other commenters unsuccessfully attempt to undermine the FCC's interpretation of Section 222. In particular, they claim that Congress' use of terms including "call" and "telephone" exchange means the statute applies only to telephone CPNI.[5] They also point to the legislative history of Section 222 and argue that it shows Congress intended Section 222 to apply only to telephone services.[6] None of these arguments are availing and the FCC should reject them.

---

[4] CTIA Comments at 16-25, 59-63; Verizon Comments at 48, 54-59; NCTA Comments at 7-14, 25; Comcast Comments at 66, 69; AT&T Comments at 100, 109; USTelecom Comments at 30, 33.

[5] CTIA Comments at 16-18; Verizon Comments at 55-56; NCTA Comments at 7-11; Comcast Comments at 66-68.

[6] *Id.*

(continued on next page)

1. Congress' use of telephone-related terms in Section 222 does not foreclose its application to broadband services

CTIA cites several subsections of Section 222 that use terms such as "call," "call location information," and "local exchange carrier."[7] The mere presence of these terms in these sections does not prove that the entire statute was meant to apply only to telephone services. CTIA's argument ignores completely that the statute applies broadly to "telecommunications carrier[s],"[8] a term that is repeated throughout the statute.[9] "Telecommunications carrier" is expressly defined in 47 U.S.C. § 153(51), and the reclassification of broadband as a telecommunications service under 47 U.S.C. § 153(53) was recently upheld by the D.C. Circuit.[10] It is presumed that use of a defined term retains its definition unless there is proof otherwise.

Congress' use of narrower terms in limited sections of Section 222 is not proof it intended to narrow the statute to phone services only. In the mid-nineties, when the Telecommunications Act was written, Congress was of course concerned with incumbent telephone services given their ability to use the data they collected in routing traffic to gain competitive advantages and target specific consumers.[11] However, Congress' concerns over some specific telephone issues does not freeze the entire statute in time, nor did those specific concerns narrow the statute to telephone services ever after. If Congress had intended to write a statute that applied to telephone services only, it could have easily done so. Congress clearly

---

[7] CTIA Comments at 16.
[8] 47 U.S.C. § 222(a); § 222(c)(1); § 222(h)(1).
[9] § 222(b)-(e), § 222(g).
[10] *U.S. Telecom Ass'n v. FCC*, No. 15-1063, 2016 WL 3251234 (D.C. Cir. June 14, 2016).
[11] Harold Feld, et al., *Protecting Privacy, Promoting Competition* at 10-11 (2016).

(continued on next page)

knew how to use terms that applied only to telephones.[12] It did not here, instead opting to use the broader term "telecommunications carriers," a term defined by the statute, allowing the FCC to classify services as such when the need arises. The FCC did just that to broadband in the Open Internet Order.[13]

CTIA's arguments about Section 230's use of the term "internet" similarly fail.[14] In Section 230, Congress was addressing a specific problem: internet platforms being held liable for the speech of their users. Platform liability was an issue specific to the internet, and therefore Congress used internet-specific language. However, the mere fact that Congress used "internet" in another section of the Telecommunications Act, yet did not use it in Section 222, does not mean Section 222 applies only to telephone services. As described above, Section 222 applies broadly to "telecommunications carriers" and services, whether those services include telephone service, broadband service, or another service so classified. Congress was under no obligation to use the term "internet" in Section 222; instead, Congress allowed the FCC to interpret what services were properly classified as a telecommunications services and therefore should be subject to the requirements of Section 222.

Additionally, the information collection capabilities of internet providers were primitive when Congress passed Section 222 and therefore the internet likely was not front-and-center on the collective minds of Congress. In 1996, monitoring

---

[12] *See U.S. Telecom Ass'n v. FCC*, No. 15-1063, 2016 WL 3251234, *23-24 (D.C. Cir. June 14, 2016) (refusing to read the term "telephone" into the defined term "public switched network").

[13] *Protecting and Promoting the Open Internet*, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd 5601, 5743 ¶ 331 (2015).

[14] CTIA Comments at 17.

(continued on next page)

technologies were nascent and, as a result, ISPs "lacked the computing horsepower to analyze and capture information quickly enough" to completely monitor the network.[15] Since then, computing technology has improved significantly to the point that complete monitoring (data collection, storage, and manipulation) is now common, thus creating the single biggest threat to user privacy.[16] Congress was not legislating against today's factual backdrop, where ISPs can monitor everyone's internet traffic, but Congress left the statute broad enough that the FCC could address that issue.

2. The data collected by BIAS providers in connection with providing broadband service meets the "solely by virtue of" requirement in Section 222(h)(1)(A)

CTIA argues that because other entities in the online ecosystem collect and maintain similar information as CPNI and PII, that it is no longer made available "solely by virtue of the carrier-customer relationship," as required by Section 222(h)(1)(A). CTIA makes the general argument that "numerous third parties regularly obtain much of the same data to which ISPs have access by virtue of the carrier-customer relationship."[17]

Whether other online entities have access to this information is irrelevant to the statutory determination.[18] Section 222 defines CPNI as "information that relates

---

[15] Paul Ohm, *The Rise and Fall of Invasive ISP Surveillance*, 2009 U. Ill. L. Rev. 1417, 1427 (2009).

[16] *Id.* at 1420 ("nothing in society poses as grave a threat to privacy as the ISP, not even Google.").

[17] CTIA Comments at 21.

[18] There is already evidence in the record that ISPs have a unique position and have access to much more information than any online ad network. *See* Center for Digital Democracy Comments at 6-10; OTI Comments at 3; Upturn Comments at 5-8; Public Knowledge Comments at 6-11.

to . . . and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship." CTIA wrongly focuses on the word "solely" and ignores the language surrounding it. The statute requires that the information be "made available *to the carrier by the customer*" solely by virtue of the relationship. The mere fact that third parties have access to similar or even identical information does not factor into the statute because that information was not provided *to the carrier by the customer.* Only in the ISP context is the statute's criteria met.[19]

3. The FCC has ample authority for its proposed definition of "customer proprietary information"

CTIA also argues that "proprietary" means information that is competitively sensitive.[20] As an initial matter, Congress deliberately declined to define "proprietary" in the context of the statute, thereby leaving its meaning vague and open to interpretation by the FCC.[21]

But even if the FCC were to limit its definition of "proprietary" to information that is competitively sensitive, CPNI and PII would easily fall within the definition. CPNI and PII are exactly the type of information that would give BIAS providers a significant competitive advantage over other business entities across a range of industries. BIAS providers that could use CPNI and PII for non-

---

[19] CTIA Comments at 20.

[20] CTIA Comments at 20. In other areas of CTIA's comments, it argues that "Congress was concerned that '[incumbent c]arriers already in possession of CPNI could leverage their control of CPNI in one market to perpetuate their dominance as they enter other service markets.'" CTIA Comments at 33. As discussed in this section, Congress' concern is just as prevalent in BIAS.

[21] *See City of Arlington, Tex. v. FCC*, 133 S. Ct. 1863 (2013); *Chevron v. Nat'l Resources Defense Council, Inc.*, 467 U.S. 837 (1984).

service-related purposes would gain an unfair advantage in advertising over other online advertisers, and certainly advertising start-ups.

BIAS providers could also use data about customers' online communications and behavior to thrust themselves into any other market where competitors normally must pay for intelligence about and access to target audiences. For example, a BIAS provider with an interest in entering the home security market could quickly build a precisely targeted list of prospective clientele for itself by determining which of its customers has internet-connected home security devices installed (likely even what those devices are), and what subset of those customers has been perusing the websites of other security companies. A BIAS provider entering the video streaming market could determine what streaming service(s) each customer already subscribes to, how much and when the customer uses various services, and, based on browsing habits, which programs the customer is or likely would be interested in. A BIAS provider launching a computer hardware company could tell what devices its customers use, when those devices begin to be less used, when customers are visiting tech support web portals, and when customers are browsing Micro Center or Fry's Electronics for new hardware. Thus, "proprietary" data should not be limited to "competitively sensitive" data.

4. Sections 222(a) and 222(c) are separate grants of authority

CTIA and others argue that Section 222(a) is not an independent grant of authority—that Section 222(c) describes how the section relates to customers.[22] This

[22] CTIA Comments at 25-26; *see also* Verizon Comments at 53-59; NCTA Comments at 14-18; Comcast Comments at 71-74.

is wrong. To read Section 222(a) as having no force and effect to information other than CPNI would completely eviscerate the meaning of Section 222(a) altogether. Where two provisions contradict, the general provision should not be read to supersede the specific provision. But where there is no conflict, "effect shall be given to every clause and part of a statute."[23]

Here, the correct result is to read Section 222(a) to govern customer proprietary information other than CPNI, rather than reading Section 222(a) out of the statute entirely. CTIA already filed a Petition for Partial Reconsideration in the Lifeline docket containing many of the same arguments against the application of Section 222(a) as it makes in this docket. They were not persuasive in that docket, and are not persuasive here. For a deeper explanation why, see OTI's Opposition to that Petition for Partial Reconsideration, filed here as an attachment to this filing.

5. Congress' use of "personally identifiable information" in other statutes does not preclude the FCC from protecting it under Section 222

CTIA argues that Congress' use of "personally identifiable information" in other statutes, while the phrase does not appear in Section 222, means the statute cannot encompass PII. This argument is not persuasive.

There is no indication that Congress intended to foreclose the FCC's ability to protect PII collected by BIAS providers. It is equally as likely as CTIA's argument, probably more likely, that Congress, knowing full-well what PII was, used inclusive language in Section 222(a) and 222(c) to fully encompass PII. Using broad language meant Congress did not have to specifically list what information it meant to

[23] *RadLAX Gateway Hotel, LLC v. Amalgamated Bank*, 132 S. Ct. 2065, 2070-72 (2012) (quoting *D. Ginsberg & Sons, Inc. v. Popkin*, 285 U.S. 204, 208 (1932)).

include, and thus it allowed the FCC, as the expert agency, to protect all relevant and appropriate data. Either way, Congress ensured that the FCC had the ability to address both CPNI and PII.

In particular, CTIA argued "Congress was concerned that '[incumbent c]arriers already in possession of CPNI could leverage their control of CPNI in one market to perpetuate their dominance as they enter other service markets.'"[24] This is exactly the type of concern the FCC, and the public, have here. BIAS providers' privileged position as intermediaries between the user and the internet allows them to collect a significant amount of private, personal information about their users that is all highly accurate. Using this data for any number of purposes, including advertising, would give incumbent BIAS providers a sizeable advantage over other advertisers.[25]

6. There is no such category as "non-individually identifiable CPNI" in Section 222

OTI joined a number of other consumer and privacy advocates in a 2012 filing that argued that CPNI that does not meet the statutory definition of "aggregate" is "individually identifiable" for purposes of applying Section 222. As it did in response to that filing, CTIA again argues that Congress intended to create a third, secret, and unregulated category of CPNI called "non-individually identifiable CPNI."[26] CTIA is reading words into the statute that are not there. As stated in previous filings, Section 222 unequivocally cannot be interpreted to

---

[24] CTIA Comments at 33.
[25] *See supra* Section I.A.3.
[26] CTIA Comments at 36-37; *see also* Verizon Comments at 44-45; NCTA Comments at 69; Comcast Comments at 84-86.

(continued on next page)

silently establish this unmentioned category of completely undefined and unregulated customer information.[27] Nothing has changed between 2012 and now to support CTIA's reading of the statute.

It is quite clear in the statute that Congress contemplated two dichotomous categories of CPNI: "individually identifiable" and "aggregate." CPNI is "individually identifiable" if it is not "aggregate," and vice versa. There is nothing in the statute to suggest otherwise. As OTI and others previously explained,

> The presentation of aggregate customer information in paragraph [222(c)](3) as contrasting with individually identifiable CPNI in paragraph [222(c)](1) indicates that all CPNI is either individually identifiable (and subject to the restrictions on use and sharing) or aggregate (and not subject to the restrictions). Thus CPNI will be considered individually identifiable unless it is aggregate.
>
> The definition of "aggregate customer information" also indicates that CPNI that is not aggregate is individually identifiable. First, aggregate information is defined in the statute, whereas individually identifiable is not. This suggests that aggregate information is a narrow carve-out category of CPNI, whereas individually identifiable information is broader. Second, the text of the definition is telling . . . . For information to be considered aggregate, both individual customer identities and characteristics must have been removed. The definition refers to both, indicating

---

[27] *In re Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers Without Customers' Consent Violates Section 222 of the Communications Act*, Petition for Declaratory Ruling of Public Knowledge, Benton Foundation, Center for Digital Democracy, Center for Media Justice, Chris Jay Hoofnagle, Common Cause, Consumer Action, Electronic Frontier Foundation, Electronic Privacy Information Center, Free Press, New America's Open Technology Institute, and U.S. PIRG, WC Docket No. 13-306 (Dec. 11, 2013) ("PK et al. Petition"); *In re Petition of Public Knowledge et al. for Declaratory Ruling Stating that the Sale of Non-Aggregate Call Records by Telecommunications Providers Without Customers' Consent Violates Section 222 of the Communications Act*, Reply Comments of Public Knowledge, et al. (Mar. 4, 2014) (PK et al. Petition Reply Comments).

(continued on next page)

> that both are sensitive. Thus a dataset from which customers' names and phone numbers have been removed but in which individual characteristics have been left intact does not meet the definition of aggregate customer information and is individually identifiable.
>
> Non-aggregate call records that contain individual characteristics—such as the call detail record of an individual customer—are individually identifiable CPNI. This remains the case even after a carrier has "anonymized" or "de-identified" the records by removing some personally identifying details. As long as individual customer characteristics remain intact in call records, they are not "aggregate" under Section 222 and are therefore individually identifiable CPNI.[28]

Any other reading of the statute would produce absurd results:

> If de-identified customer records were neither individually identifiable CPNI under 222(c)(1) nor aggregate customer information under 222(c)(3), carriers' use of those records would be even less regulated than their use of aggregate customer information, even though aggregate records are more privacy protective than non-aggregate de-identified records. Section 222(c)(3) requires carriers that use, disclose, or permit access to aggregate customer information other than for purposes described in 222(c)(1) to "provide[] such aggregate information to other carriers or persons on reasonable and nondiscriminatory terms and conditions upon reasonable request therefor." Aggregate customer information is "collective data that relates to a group or category of services or customers, from which individual customer identities *and characteristics* have been removed." Because records de-identified . . . [may] leave intact individual characteristics such as ZIP code, call times and durations, and locations, they are not aggregate. Therefore if carriers were correct that de-identified customer information is not individually identifiable CPNI, they could share such records while escaping Section 222(c)(3). In other words, records from which individual identities had been removed could be shared with third parties with impunity. In contrast, records from which individual identities and characteristics had been removed could be shared with third parties only if it were also made available on a

[28] PK et al. Petition at 5-6.

(continued on next page)

> nondiscriminatory basis to other carriers and persons. This would truly be an absurd result, and as Sprint points out, interpretations of a statute that would produce absurd results are to be avoided.[29]

Even if the Commission nevertheless accepted CTIA's assertion that the statute somehow creates a third category of data *sub silentio*, there are important reasons to protect pseudonymous data. Primarily, re-identification techniques have become very effective in recent years, and re-identifying datasets is now trivial.[30] Specifically, "researchers have found data fingerprints in non-PII data, with much greater ease than would have been predicted," citing examples that use health records, historical location data, and web search queries.[31] In several studies, researchers have identified individuals from so-called anonymous datasets by taking advantage of what computer scientist and Professor Paul Ohm terms "pockets of surprising uniqueness."[32] In a classic example, Arvind Narayanan and Vitaly Shmatikov identified individual Netflix users based on their movie choices and how they rated those movies.[33] Recently, another research team was able to

---

[29] PK et al. Petition Reply Comments.

[30] Researchers have repeatedly demonstrated how easy it is to identify individuals using seemingly innocuous, non-PII data contained in large data sets. *See* Latanya Sweeney, *k-Anonymity: A Model For Protecting Privacy*, 10 Int'l J. Uncertainty, Fuzziness & Knowledge-Based Sys. 557, 570 (2002); Latanya Sweeney, *et al.*, *Identifying Participants in the Personal Genome Project by Name*, Data Privacy Lab, Harvard Univ. (2013); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. Rev. 1701, 1777 (2010).

[31] Ohm, *supra* note 30, at 1723.

[32] *Id.*

[33] Arvind Narayanan & Vitaly Shmatikov, *Robust De-anonymization of Large Sparse Datasets*, *in* Proceedings of the 2008 IEEE Symposium on Security and Privacy 111-125 (2008); *see also* Arvind Narayanan *et al.*, *Cookies That Give You Away* (attached to letter filed by Mr. Narayanan in Dkt. 16-106, May 27, 2016, at https://ecfsapi.fcc.gov/file/60002080817.pdf).

(continued on next page)

"fingerprint" individual automobile drivers 100 percent of the time based on 90 minutes of driving data collected by the vehicle's internal computer system.[34]

The tools used for re-identification are effective and even rudimentary. Ohm describes one re-identification technique, the "inner join," in which a program such as Microsoft Excel can be used to crack anonymity by combining two databases by matching shared information.[35] Stanford researchers used this cross-referencing technique to identify individuals using only the users' phone metadata and publicly available information gathered from Yelp, Google Places, and Facebook.[36] Based on these results, the researchers concluded that "the policy distinction between PII and non-PII is not based on sound science" and "telecommunications regulation should also incorporate a scientifically rigorous understanding of the privacy properties of these data."[37]

There is no support for CTIA's argument about a secret third category of CPNI. But even if there were, that category should be considered individually identifiable as Congress intended under Section 222(c)(1).

---

[34] Andy Greenberg, *A Car's Computer Can 'Fingerprint' You in Minutes Based on How You Drive*, Wired (May 25, 2016), https://www.wired.com/2016/05/drive-car-can-id-within-minutes-study-finds (finding drivers could be identified 87% of the time with only 15 minutes of car brake pedal data).

[35] Ohm, *supra* note 30, at 1726.

[36] Jonathan Mayer, Patrick Mutchler, and John C. Mitchell, *Evaluating the Privacy Properties of Telephone Metadata*, PNAS 2015 113 (20), available at http://www.pnas.org/content/113/20/5536.full.

[37] *Id.*

(continued on next page)

7. The term "approval" in Section 222 is ambiguous and the FCC can define it

CTIA argues Congress did not intend to exclude certain types of "approval" under the statute, such as agreeing to give up data privacy in exchange for internet service, or paying more per month to protect privacy.[38] These arguments are unpersuasive.

First, the term "approval" was not defined by Congress. A statute that provides an agency authority, but which also includes ambiguous terms, necessarily provides that agency the authority to define those terms.[39] Section 222(c) states that telecommunications carriers must obtain the "approval of the customer" before engaging in certain uses of customer data. The FCC is certainly at liberty to state, and it should, that coercive practices that force customers to give up their privacy rights altogether to access the internet does not constitute "approval of the customer." In fact, it is difficult to fathom how a "take-it-or-leave-it" privacy policy is approval at all, because it is unlikely that the customer could find broadband service elsewhere.[40] The customer may not in fact approve, but may feel forced to "approve" because that customer wants access to the internet. And with seriously discounted "pay-for-privacy" policies, the BIAS provider is simply manipulating "approval" in order to goad customers into letting the BIAS provider have complete freedom with how they use their customers' data. This is neither fair nor right.

---

[38] CTIA Comments at 47; Verizon Comments at 47; NCTA Comments at 16-18; Comcast Comments at 73.
[39] *See City of Arlington*, 133 S. Ct. at 1863 (2013); *Chevron*, 467 U.S. at 837.
[40] 2016 Broadband Progress Report, 31 FCC Rcd 699, ¶ 86 (2016).

(continued on next page)

Second, the FCC is at liberty to define whether "approval" of the customer means opt-in or opt-out.[41] There, too, the statute is ambiguous and the fact that the word "approval" in Section 222(c)(1) differs from the "express prior authorization of the customer" language provided in Section 222(f) does not resolve the ambiguity. Congress had specific concerns about the authority of telecommunications carriers to use call location information, and therefore was very clear about what type of customer approval was required.[42] That elsewhere Congress used the more ambiguous term "approval" suggests only that it was content to grant the FCC greater leeway to determine what approval would suffice in other circumstances, not that it intended to specifically required the FCC to accept mere passive consent.

B. The Commission has authority under 201(b) and 202 to prohibit any practices it decides are unreasonable and unjust, including those practices discussed in the Notice

CTIA argues that Section 201(b) is limited by Section 222 and therefore cannot provide the basis for the proposed rules. In particular, CTIA argues that "data privacy and security practices related to non-CPNI customer information are not practices 'in connection with' broadband service, and thus cannot be governed by Sections 201(b) and 202"[43] and that the phrase "made available to the carrier by the customer solely by virtue of the carrier-customer relationship" further limits Sections 201(b) and 202.[44] These arguments must be rejected.

---

[41] *See* Tribe Comments at 3.
[42] 47 U.S.C. § 222(f).
[43] CTIA Comments at 61; *see also* Verizon Comments at 48-49; NCTA Comments at 25; Comcast Comments at 69-70.
[44] CTIA Comments at 62-63; *see also* Verizon Comments at 48-49; NCTA Comments at 25; Comcast Comments at 69-70.

Regarding CTIA's first argument, that Section 222 limits Section 201(b) because it constitutes a "comprehensive" privacy regime, OTI ad others fully addressed this issue in an opposition to CTIA's Petition for Partial Reconsideration of the Lifeline order. That opposition is included as an appendix to this filing. For the same reasons that OTI argued in October 2015, CTIA's arguments against privacy and data security applications of Section 201(b) should be rejected.

CTIA's attempt to label non-CPNI data privacy and security practices as not provided "in connection with" a broadband service is unpersuasive. The exact opposite is true. The broadband provider has access to the data only because the carrier is providing the customer a vital service—internet access—through which the carrier collects the customer's data. Indeed, as described above, both non-CPNI and CPNI data meet the "made available" language in Section 222(h)(1)(A).[45] In this modern era, it is unfathomable to argue that protecting and securing BIAS customer data do not follow immediately from its mere collection.

Therefore, the FCC is on firm statutory grounds to enact its broadband privacy rules and should do so without delay.

II. The proposed rule does not violate the First Amendment

Several commenters argue the FCC has proposed a rule that would violate the First Amendment rights of BIAS providers to "speak" to their customers because the rule prevents BIAS providers from engaging in the "process of gathering and analyzing data in preparation for speech," which is also protected by

[45] *Supra* at pp. 5–6.

(continued on next page)

the First Amendment.[46] Thus, these commenters argue, at least the intermediate scrutiny test from *Central Hudson* applies. Some also argue that the rule may even be subject to heightened scrutiny because the Supreme Court in *Sorrell v. IMS Health, Inc.* arguably left open that possibility.[47]

The FCC should not be persuaded by these arguments, which mischaracterize precedent and rely on unpersuasive evidence and also point to the FTC's approach as if it were the only approach available or possible. For the reasons below, the FCC's proposal does not violate the First Amendment.

A. The FCC's proposal meets First Amendment scrutiny under *Central Hudson*

Several cases have reviewed Section 222 rules and have applied the *Central Hudson* test, which is likely the same test that would be applied on review of this rule. Under the *Central Hudson* test, the First Amendment permits burdens on commercial speech only if: the speech at least concerns lawful activity and is not misleading, the governmental interest is substantial, the regulation directly advances the governmental interest asserted, and the regulation is not more extensive than necessary to serve that interest.[48] The first is not at issue, so these comments will address the other elements of the test.[49] Last, contrary to what some

---

[46] Tribe Comments at 3 (filed by CTIA, NCTA, and USTelecom as a "letter" in Dkt. 16-106 on May 27, 2016); CTIA Comments at 76-78; Verizon Comments at 29-40, 50-53; NCTA Comments at 32-33; Comcast Comments at 90.

[47] Tribe Comments at 13.

[48] *NCTA v. FCC*, 555 F.3d 996, 1000 (D.C. Cir. 2009).

[49] Commenters have asserted that the "canon of constitutional avoidance requires that the FCC narrowly construe its authority." Tribe Comments at 38. This argument is confounding, given that the canon of constitutional avoidance states that "a case should not be resolved by deciding a constitutional question if it can be resolved in

(continued on next page)

have argued, the FCC's proposal would not be subject to heightened scrutiny under *Sorrell v. IMS Health, Inc.*

1. The FCC has a substantial government interest in protecting consumer privacy

The FCC has a clear substantial government interest in this case. Protecting consumer privacy has already been held to constitute a substantial government interest by multiple courts. Even if it were not already recognized as such, consumers care deeply about their privacy and thus the government should protect it in whatever ways it can. Further, privacy violations result in significant harm to consumers, providing more support for the FCC's proposed rule.

a. Multiple courts have determined protecting consumer privacy to be a substantial government interest

Commenters agree that there is a substantial governmental interest in protecting privacy.[50] But even if this point were contested, the Commission can be confident that the government's interest in protecting privacy justifies regulation; indeed several important cases have held that protecting consumer privacy is a substantial government interest.[51] For example, the Supreme Court has stated that

---

some other fashion." *Constitutional-Avoidance Rule*, Black's Law Dictionary (10th ed. 2014). The canon does not even apply to agencies, it applies to courts.

[50] CTIA Comments at 81 (citing *NCTA v. FCC*, 555 F.3d at 1001; *U.S. West Inc. v. FCC*, 182 F.3d 1224, 1234-35 (10th Cir. 1999); *Trans Union Corp. v. FTC*, 267 F.3d 1138, 1142 (D.C. Cir. 2001) (*Trans Union II*)).

[51] *NCTA v. FCC*, 555 F.3d at 1001; *U.S. West*, 182 F.3d at 1234-35; *Trans Union II*, 267 F.3d at 1142; *see also Gomez v. Campbell-Ewald Co.*, 768 F.3d 871, 876 (9th Cir. 2014) (protection of cell phone privacy is a substantial government interest).

(continued on next page)

"both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person."[52] The Court in *Sorrell* also stated "[p]rivacy is a concept . . . integral to the person and . . . essential to freedom."[53] From these cases it is clear the Court recognizes privacy as important to our society and that the government can play a role in establishing privacy requirements.[54]

Multiple courts of appeals have also recognized the importance of privacy specifically in the Section 222 context. The Tenth Circuit in *U.S. West v. FCC* stated Section 222 had a "specific and dominant purpose" in "the protection of customer privacy."[55] Among its reasons for believing so, the court said "the plain language of the section deals almost exclusively with privacy," the statute is titled "Privacy of customer information," and the statute is replete with references to privacy and confidentiality of customer information.[56] In *NCTA v. FCC*, the D.C. Circuit upheld opt-in rules under Section 222 and, dismissing First Amendment arguments, stated "we have already held, in an analogous context, that 'protecting the privacy of consumer credit information' is a 'substantial' government interest."[57] In the prior

---

[52] *U.S. Dept of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989) (cited in *NCTA v. FCC*, 555 F.3d at 1001).
[53] *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 579 (2011).
[54] *Id.* ("The capacity of technology to find and publish personal information, including records required by the government, presents serious and unresolved issues with respect to personal privacy and the dignity it seeks to secure. In considering how to protect those interests, however, the State cannot engage in content-based discrimination to advance its own side of a debate.").
[55] *U.S. West*, 182 F.3d at 1236.
[56] *Id.*
[57] *NCTA v. FCC*, 555 F.3d at 1001 (citing *Trans Union Corp. v. FTC*, 245 F.3d 809, 818 (D.C. Cir. 2001) (*Trans Union I*)) ("we have no doubt that this interest—protecting the privacy of consumer credit information—is substantial.").

(continued on next page)

case to which it referred, the D.C. Circuit dismissed similar First Amendment arguments by looking to the Congressional findings and purpose of the Fair Credit Reporting Act, which stated "[t]here is a need to insure that consumer reporting agencies exercise their grave responsibilities with . . . respect for the consumer's right to privacy."[58] Given the Tenth Circuit's analysis, Section 222 had a similar purpose and motivation.

Courts have even shown an affinity for broad privacy interests. While the court in *U.S. West* presumed the FCC meant to protect simply "embarrassing" information from being disclosed publicly, the D.C. Circuit in *NCTA v. FCC* understood the interest in protecting privacy not to be that narrow. The D.C. Circuit concluded "[t]here is a good deal more to privacy than [embarrassment]. It is widely accepted that privacy deals with determining for oneself when, how and to whom personal information will be disclosed to others."[59] Thus, while opponents to the Commission's privacy proposal continue to claim that privacy interests and harms are difficult or impossible to define,[60] there has been a steady growth of

---

[58] *Trans Union I*, 245 F.3d at 818.

[59] *NCTA v. FCC*, 555 F.3d at 1001 (citing Daniel J. Solove, *Conceptualizing Privacy*, 90 Cal. L. Rev. 1087, 1109-10 (2002)). *See also id.* ("both the common law and the literal understandings of privacy encompass the individual's control of information concerning his or her person.") (quoting *Reporters Comm. for Freedom of the Press*, 489 U.S. at 763).

[60] For examples of the myriad harms caused by privacy violations, see Daniel Solove, *A Taxonomy of Privacy*, 154 U. Pa. L. Rev. 477, 490 (2006) (establishing a new taxonomy of privacy hams that include information collection, information processing, information dissemination and invasion); M. Ryan Calo, *The Boundaries of Privacy Harm*, 86 Ind. L. J. 1131, 1133 (2011) (developing a system that separates privacy harms into two categories: subjective privacy harms and objective privacy harms); Kelsey Finch, *The Evolving Nature of Consumer Privacy Harm*, IAPP (Apr. 1, 2014), https://iapp.org/news/a/the-evolving- nature-of-consumer-privacy- harm/ (explaining the FTC views privacy harms under Section

(continued on next page)

understanding in several courts, including the Supreme Court, that the protection of one's privacy is fundamental and the ability to choose when others collect, use, and disclose that information is integral to a person.

Based on these cases, it is clear the FCC has a substantial interest in protecting consumer privacy as against their BIAS providers who have uninterrupted and comprehensive access to almost all data relating to their customers.

The court in *U.S. West* did state, however, that "privacy may only constitute a substantial state interest if the government specifically articulates and properly justifies it" through building an adequate record.[61] The record here contains plenty of evidence that protecting consumer privacy is a substantial government interest.

b. Consumers care about privacy and require government intervention to ensure they have control over how their information is used

The government also has a substantial interest in protecting consumer privacy because consumers care deeply about their online privacy and need more control over how their information is used than the market alone can deliver.[62] The internet has become an integral aspect of nearly every sphere of daily life. As users continue to reveal more personal information about themselves through their activity online (almost all of which is visible to BIAS providers), concern has grown

---

5's "unfairness" prong and considers "nonmonetary, abstract, autonomy and dignitary-based harms").

[61] *U.S. West*, 182 F.3d at 1235.

[62] Even though most research and surveys have been conducted regarding online privacy generally, the conclusions can readily be applied to BIAS providers.

(continued on next page)

that this information may be used in ways that violate privacy. In a November 2015 poll by Freedman Consulting, over eighty percent of Americans said they were concerned about their online privacy, including fifty percent that were "very concerned."[63] In the 2016 Consumer Privacy Index (CPI) conducted by TRUSTe, 43% of US internet users indicated they were more concerned about their privacy than one year prior.[64]

Notwithstanding their clear desire for increased privacy, consumers currently cannot retain sufficient control of online data to avoid suffering perceived privacy violations. Consumers do not like what is happening to their data online and they often feel violated, annoyed, or intruded upon when companies make exploitative use of or sell their data. For instance, the CPI reported that consumers were more concerned about not knowing how personal information was collected online (68%) than about losing their principal income (57%).[65] In response to a 2016 Pew survey, respondents "regularly expressed anger about the barrage of unsolicited emails, phone calls, customized ads or other contacts that inevitably arises when they elect to share some information about themselves."[66] Pew concluded that consumer views of privacy versus sharing information depends on

---

[63] Freedman Consulting, *Poll Finds Strong Support for Expanding Online Privacy Protections and Internet Access* (Nov. 23, 2015), available at https://tfreedmanconsulting.com/wp-content/uploads/2016/02/PrivacyandAccessResearchFindings_151123.pdf.
[64] TRUSTe/National Cyber Security Alliance, *U.S. Consumer Privacy Index 2016*, TRUSTe (Dec. 2015), https://www.truste.com/resources/privacy-research/ncsa-consumer-privacy-index-us/.
[65] *Id.*
[66] Lee Rainie & Maeve Duggan, *Privacy and Information Sharing*, Pew Research Center (Jan. 14, 2016), http://www.pewinternet.org/2016/01/14/privacy-and-information-sharing/.

(continued on next page)

the context: "people indicated that their interest and overall comfort level depends on the company or organization with which they are bargaining and how trustworthy or safe they perceive the firm to be."[67] In another study, Bain & Company

> surveyed more than 900 U.S. consumers and found that 91 percent of respondents do not want companies selling their data, even if they are compensated for it. People opposed to having their data used or shared—even when asked—are rarely swayed by offers of monetary compensation. Moreover, the reluctance to trade their data for monetary compensation applies to all customers, no matter how active or sophisticated they are online.[68]

Consumers also show an aversion to mere use of data for targeted advertising purposes.[69] Clearly, consumers are upset by the lack of control and transparency over how information is used, disclosed, and sold.

---

[67] *Id.* Thus, not only does this support the FCC's proposal to give consumers more control over their data when it comes to BIAS providers, it also seriously undermines opponents' nonsensical arguments that consumers will be confused by different privacy regimes for BIAS providers and content companies. Consumers already understand that different companies have different levels of trust and take that into account when determining if, when, and how to disclose data.

[68] Bain & Company Press Release, *How can companies acquire customer data while building customer loyalty at the same time? Ask permission*, Bain & Company (May 11, 2015), http://www.bain.com/about/press/press-releases/Digital-privacy-survey-2015-press-release.aspx.

[69] Joseph Turow et al., *Americans Reject Tailored Advertising and Three Activities that Enable It* 8, 13 (2009), https://www.asc.upenn.edu/news/Turow_Tailored_Political_Advertising.pdf (based on nationwide survey, 66% of Americans do not want marketers to tailor advertisements to their interests; 68% of Americans "definitely" would not allow websites to track them anonymously even when that is disclosed). This provides a concrete rebuttal, based on actual evidence rather than conjecture, to Tribe's unsupported argument that "merely using . . . information already in [the ISP's]

(continued on next page)

Consumers even feel powerless against the data practices of the companies with which they interact directly. Joseph Turow, a privacy expert, professor, and researcher at the University of Pennsylvania, conducted a study that found consumers feel "resigned to the inevitability of surveillance and the power of marketers to harvest their data."[70] These consumers "believe it is futile to manage what companies can learn about them."[71] Turow's study found that "more than half do not want to lose control over their information but also believe this loss of control has already happened."[72] Similarly, a 2014 Pew survey found that "91% of adults "agree" or "strongly agree" that "consumers have lost control over how personal information is collected and used by companies."[73] This is certainly true with ISPs, where consumers have even less choice over alternatives.

Consumers simply do not know how to protect themselves from perceived privacy violations. The Freedman survey showed that 61% of Americans "say they are concerned [about privacy] but don't know what to do to protect themselves. Communities of color are especially likely to feel this way, with 73% of Latinos and

---

possession to serve consumers with more rather than less relevant advertising" does not cause harm." Tribe Comments at 20.

[70] Joseph Turow et al., *The Tradeoff Fallacy* (Report from the Annenberg School for Communication, June 2015), available at https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf.

[71] *Id.*

[72] *Id.* This resignation could explain in part why consumers care deeply about privacy but may also give it up for what seems to be a low price. *See e.g.*, Jens Grossklags & Alessandro Acquisti, *When 25 Cents is too much: An Experiment on Willingness-To-Sell and Willingness-To-Protect Personal Information* (2007), http://people.ischool.berkeley.edu/~jensg/research/paper/Grossklags_Acquisti-WEIS07.pdf.

[73] Mary Madden, *Few Feel that the Government or Advertisers can be Trusted*, Pew Research Center (Nov. 12, 2014), http://www.pewinternet.org/2014/11/12/few-feel-that-the-government-or-advertisers-can-be-trusted/.

(continued on next page)

66% of African and Asian Americans agreeing with this sentiment."[74] This may be in part because privacy policies are long, legalistic, and unclear, which explains why 94% of respondents to the Freedman survey supported "[r]equiring companies to post a short, clear written disclosure box on their homepage that explains how your information will be used."[75]

One of the few ways in which consumers know to protect their privacy is by avoiding certain online activities altogether. A recent study from the National Telecommunications and Information Administration (NTIA) found that the fear of becoming a victim of a privacy breach stopped forty-five percent of online households from "conducting financial transactions, buying goods or services, [or] posting on social networks."[76] The CPI echoed these concerns: 74% of respondents have limited their online activity in the last year due to privacy concerns, 36% have stopped using certain websites, 29% have stopped using an app, many of whom said this was because the sites and apps asked the consumer to provide too much information.[77] That same survey showed that, for privacy reasons, consumers have refrained from clicking on ads (51%), have withheld personal information (44%), have not downloaded particular apps or products (32%), and have stopped an

---

[74] Freedman Consulting, *supra* note 63.
[75] *Id.*
[76] Rafi Goldberg, *Lack of Trust in internet Privacy and Security May Deter Economic and Other Online Activities*, NTIA Blog (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internet-privacy-and-security-may-deter-economic-and-other-online-activities. *See also* Stephen Cobb, *Privacy and security fears—predictability—impact US online commerce*, We Live Security (May 16, 2016), http://www.welivesecurity.com/2016/05/16/privacy-and-security-fears-impact-online-commerce/ (stating economists and sociologists should have anticipated the NTIA's findings).
[77] TRUSTe/National Cyber Security Alliance, *supra* note 64.

(continued on next page)

online transaction (28%).[78] Unfortunately, while consumers can generally avoid using most apps or otherwise limit what information a website can see,[79] they cannot avoid their BIAS provider if they want to get online in the first place.

For these and many more reasons, consumers need more control over their data and easier tools to protect their privacy than the market alone can deliver. From the CPI, consumers want control over who has access to personal information (45%), how the personal information is used (42%), the type of info collected (41%), and 23% want to be able to delete personal information after its collection.[80] Not only do these results undermine the so-called "notice fatigue" argument, but they also comport with Alan Westin's privacy definition of *Privacy and Freedom*: "[p]rivacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."[81] This would require actual control and options for consumers to protect their data not only from the "first party" collector but also how that first party shares the data with other parties. The FCC's rule would provide such protections.

Consumers recognize that only regulatory intervention can restore privacy—and that's exactly what they are clamoring for. A whopping 78% of internet users believe that the federal government should "take an active role in protecting online privacy," according to the Freedman survey.[82] Bain research found that "[a] full two-thirds [of consumers] feel that it should be illegal for companies to collect or

---

[78] *Id.*
[79] OTI Comments, at 5-6.
[80] TRUSTe/National Cyber Security Alliance, *supra* note 64.
[81] Alan F. Westin, Privacy and Freedom 7 (1967).
[82] Freedman Consulting, *supra* note 63.

(continued on next page)

use such data without getting prior consent."[83] And 64% of respondents to a 2014 Pew survey "believe[d] the government should do more to regulate advertisers."[84]

All of this evidence combines to establish, unmistakably, that the government has a clear and substantial interest in protecting consumer privacy. Consumers are concerned about their privacy, they want increased choices regarding their data, and they want government to help. Without government help, some consumers will even censor their online activities to the detriment of the entire internet ecosystem. The Commission has the authority to protect consumers against the actors with the most problematic and invasive window into private online activities: BIAS providers.[85]

c. Privacy violations lead to serious consumer harms

There is mounting evidence that expansive data collection, use, and disclosure practices harm consumers. Not only do privacy violations lead to concrete harms, but the definition of "privacy harm" is constantly evolving, with subjective concerns becoming more prevalent.

Privacy harms exist at collection, use, and disclosure of data. According to the oft-cited taxonomy of privacy harms developed by Daniel Solove, a prominent privacy scholar, consumers experience harm when information is collected, processed, and disseminated.

---

[83] Bain & Company Press Release, *supra* note 68.
[84] Mary Madden, *supra* note 73.
[85] Ohm, *supra* note 15, at 1420-21.

(continued on next page)

"The collection of [personal] information itself can constitute a harmful activity," Solove explained.[86] When information is constantly collected, people are being constantly surveilled.[87] Constant surveillance "has problematic effects" such as creating "feelings of anxiety and discomfort."[88] Awareness of even of the possibility of constant surveillance can cause a person to "alter her behavior," which leads to "self-censorship and inhibition."[89] In the context of online communications, this particular ill effect has already manifested itself as shown by the NTIA study and the CPI referenced above, and constitutes a harm to the individual, to businesses adversely affected, and to society as a whole as internet use is chilled.

Information processing, referring to the use, storage, and manipulation of collected data, provides another opportunity for harm. Processing of information can take many forms. One way to process information is to "aggregate," or combine, data from disparate datasets that have information about the same individual. This type of combination "reveals facts about data subjects in ways far beyond anything they expected when they gave out the data . . . . The dossier created by aggregating a person's data is often used as a way to judge her."[90]

---

[86] Solove, *supra* note 60, at 488.
[87] *Id.* at 493.
[88] *Id.*
[89] *Id.*; *see also id.* at 494 ("Paul Schwartz argues that surveillance inhibits freedom of choice, impinging upon self-determination.") (citing Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 Vand. L. Rev. 1609, 1656 (1999)); *id.* at 495 (referencing the "Panoptic effect").
[90] *Id.* at 507-508 (citing *U.S. Dept of Justice v. Reporters Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989), where the Court differentiated between "scattered disclosure of the bits of information contained in the [criminal] rap sheet and revelation of the rap sheet as a whole").

(continued on next page)

Combining data about people into digital dossiers is a well-documented practice of marketers.[91] These dossiers are used to provide sometimes very intrusive marketing and advertising to particular customers based, potentially, on household income (payday loans) or race (junk food?).[92]

Insecurity is the harm of "being placed in a weaker state, of being made more vulnerable to a range of future harms."[93] This is a harm separate from the future harm that would later occur, such as a data breach, identity theft, or disclosure of private financial data.[94] In essence, the harm is caused by "[t]he careless use of data by businesses."[95]

Secondary uses are another practice that causes harm. Using data in ways the consumer does not consent to leads to dignitary harm and violates expectations, which reduces trust between the individual and the entity responsible for the data misuse, and may cause the individual to experience fear, uncertainty, powerlessness, and vulnerability.[96] Consumers may feel that they would not have agreed to divulge data if they knew about all the potential uses to which it would be put.[97] Particularly with BIAS providers, a customer may lose trust in their broadband provider, leading to severe chilling effects.

Exclusion, "the failure to provide individuals with notice and input about their records,"[98] similarly causes harm. Not allowing users to have control over

---

[91] Solove, *supra* note 60, at 508.
[92] *Id.*
[93] *Id.* at 518.
[94] *Id.* at 515-517.
[95] *Id.* at 516.
[96] *Id.* at 520.
[97] *Id.*
[98] *Id.* at 521.

(continued on next page)

their data profiles reduces accountability for the companies maintaining that information. Again, this lack of being informed about and not being able to do anything to affect how data is being used causes "a sense of vulnerability and uncertainty in individuals."[99] When information is increasingly being used to make decisions that affect our lives (including what is included in credit reports[100] and whether a person gets a loan[101]), this vulnerability matters.

Finally, information dissemination is the harm that most people are familiar with, though as discussed above, it is not the only type of harm that exists.[102] For that reason, this type of harm needs little explanation. In short, there are several harms that come about from disseminating information, including breaching confidentiality after one party promised to keep information confidential,[103] disclosing truthful information about a person that affects the way others judge her character,[104] appropriating another's information for your own gain,[105] and disseminating false or misleading information about a person.[106]

Other scholars have also described privacy harms. Ryan Calo, another privacy scholar, has devised a "subjective" and "objective" harms dichotomy.[107] Calo's harms are similar to Solove's harms and therefore do not require extensive

---

[99] *Id.*
[100] *Id.* at 508.
[101] *Id.*
[102] *NCTA v. FCC*, 555 F.3d at 1000 ("the carrier's sharing of customer information with a joint venturer or an independent contractor without the customer's consent is itself an invasion of the customer's privacy.").
[103] Solove, *supra* note 60, at 526.
[104] *Id.* at 530-36.
[105] *Id.* at 545.
[106] *Id.* at 549.
[107] M. Ryan Calo, *supra* note 60, at 1131.

(continued on next page)

discussion. However, "subjective privacy harms are those that flow from the perception of unwanted observation. . . . They can range in severity from mild discomfort at the presence of a security camera to 'mental pain and distress far greater than could be inflicted by mere bodily injury.'"[108] Similarly, they can be associated with "embarrass[ment]" or "an ongoing sense of regret."[109] More generally, it is prolonged, excessive, and unwanted "psychological arousal" that can be harmful.[110] Calo, like Solove, states constant monitoring need not be actual, merely believed, for harms such as embarrassment, chilling effects, and loss of solitude, to apply.[111] Calo's objective harms have to do with the real-world consequences of constant observation, including data breaches, identity theft, or using specific personal data to serve someone an ad. "The problem arises when, as often, an individual has no idea that the information was even collected or, if she does, how it will be used."[112]

All of these harms apply equally, if not more so, in the BIAS provider context. Given BIAS providers' ability to see nearly every activity their users engage in online, their information is comprehensive and could be used in any number of ways.[113] This constant surveillance could cause serious harms to customers and the

---

[108] *Id.* at 1142 (quoting Samuel Warren & Louis Brandeis, *The Right to Privacy*, 4 Harv. L. Rev. 193, 196 (1890)).
[109] *Id.* at 1144.
[110] *Id.* at 1147-48.
[111] *Id.* at 1146-47
[112] *Id.* at 1149.
[113] To the extent Tribe bases his First Amendment arguments on claims made in the Swire paper that ISPs do not have access to basic data about their customers, there is evidence in the record showing the Swire paper is misleading or not telling the whole story. *E.g.*, Upturn Comments at 1. At any rate, the Swire paper *should not be* the basis for policymaking nor a First Amendment analysis given its serious weaknesses.

internet generally as customers feel threatened, which will lead to reduced internet use. It is clear that customers have lost control. This is evident in the FTC's privacy regime, which primarily protects consumers primarily when companies *deceive* consumers in their privacy policies. This, in effect, allows companies to make their own rules without input or choice from their consumers. The FCC's proposal is designed to remedy this and other problems.

The FCC is on solid ground for the first prong of the Central Hudson test. The FCC has very clear interests in protecting the privacy of BIAS provider customers.

2. The proposal materially advances these interests

Tribe and others stretch to great lengths to find reasons these proposed rules are not tailored to the FCC's substantial interest in protecting consumer privacy and giving consumers choices. But the connection is a simple one: consumers desire and need more choices about if, when, and how to divulge information to other entities to ensure those consumers feel free to use the internet uninhibited; when it comes to data collection by their BIAS provider, customers have no choice but to give that information up because of the special relationship between a carrier and the customer.[114] Thus, the only way for customers to have actual choice is to require accurate, detailed notice to customers and then to allow those customers to opt-in (or, in certain limited circumstances, opt-out), of certain uses and disclosures of data. Consumers should also decide what to do when their data is hacked or disclosed without their permission, rather than allowing the BIAS provider to act in its own best interests.

---

[114] This special relationship was explicitly recognized and protected by Congress under Section 222.

Tribe's first argument under this prong focuses on the supposed "under-inclusiveness" of the proposal. Primarily, he argues that this rule applies only to BIAS providers and therefore violates the First Amendment by targeting certain speakers. But this argument is without merit. The FCC has jurisdiction over BIAS providers, but not online content companies, and this is clear from Section 222.[115] The FCC lacks authority to impose such a privacy regime on online content companies. This was by design: Congress authorized the FCC to regulate (primarily) telecommunications carriers—in particular, the privacy practices of telecommunications carriers. Tribe's argument paradoxically states the FCC is powerless to protect the confidentiality of customer data unless it protects customer data on *all* online services, over which the FCC has no authority.

Another argument attempts to undermine the claim that consumers cannot avoid giving data to their broadband provider. Tribe argues this "assertion is [sic] cannot be squared with the factual record, which shows that the average internet user moves among six different devices . . . and that as much as 70% of internet traffic will be encrypted by the end of 2016."[116] Tribe makes these assertions without support. In fact, the estimate is probably closer to 4 devices.[117] Even if there were six devices, many of them are likely to be tablets, laptops, or similar devices that, while "mobile," connect to the same Wi-Fi connection that travels through the

---

[115] *See U.S. Telecom Ass'n v. FCC*, 2016 WL 3251234, at *23-24 (D.C. Cir. June 14, 2016).

[116] Tribe Comments at 25.

[117] Joseph Waring, *Number of devices to hit 4.3 per person by 2020 —report*, Mobile World Live (Oct. 16, 2014), http://www.mobileworldlive.com/featured-content/home-banner/connected-devices-to-hit-4-3-per-person-by-2020-report (predicting 4.3 devices per person by 2020).

(continued on next page)

customer's BIAS provider. It is rare for people to own more than one mobile phone.[118] Thus, only one sixth of those devices are likely to be capable of connecting to another BIAS provider. And even then, some portion of the data used on that device will be in that person's home, likely connected to the same Wi-Fi connection the other five devices are connected to. To the extent that mobile device moves beyond the home and connects solely over the customer's wireless connection, then that data is being collected by a (potentially) different provider that similarly processes it and likely uses it or sells it for advertising and other purposes. Tribe similarly argues "[t]he average user can readily switch her mobile broadband provider during a coffee break," which is similarly unsupported. Not only does finding a new plan at a new provider take serious research, but even basic requirements like switching your phone number over can take a significant amount of time.[119] And there are serious questions about placing any merit on measuring encryption adoption as a portion of total internet traffic, given that Netflix is encrypted (therefore protecting your movie preference from your BIAS provider) but WebMD is not (therefore allowing your BIAS provider to collect that data and monetize it).[120]

---

[118] International Telecommunication Union, *Mobile Cellular Subscriptions (per 100 people)*, The World Bank, http://data.worldbank.org/indicator/IT.CEL.SETS.P2?locations=US (last visited July 6, 2016) (showing U.S. having 110 mobile phones per 100 people).

[119] *See* Jonathan Leggett, *A guide to switching mobile phone providers*, uSwitch (June 7, 2016), https://www.uswitch.com/mobiles/guides/how-to-switch-mobile/; Jonathan Leggett, *Transferring your mobile number to a new phone*, uSwitch (May 18, 2016), https://www.uswitch.com/mobiles/guides/porting-your-mobile-phone-number.

[120] Upturn Comments at 3.

(continued on next page)

Tribe argues the proposal lacks tailoring (because the proposal includes restrictions on internal use of data) and distinguishes speech based on "what a marketer says."[121] These arguments fail given the important and substantial governmental interests stated above. Internal use is just as problematic for consumers as is disclosure and dissemination, and therefore the FCC is correct to give consumers choice over internal use. Similarly, it is clear from the record that the marketing-based distinction also satisfies the First Amendment because consumers resoundingly reject tailored advertising in theory, or at the very least desire a choice as to how data is used in that manner.[122]

Further, Tribe attempts to undermine the proposal by arguing it differentiates between corporate affiliates and third-party vendors and agents without reason. While OTI supports requiring opt-in for *both* corporate affiliates *and* third parties, this distinction also makes sense. Corporate affiliates are much more likely to be known and understood as part of the corporate family and thus data is more likely to be shared within those families. The FTC has stated such.[123] Third parties, such as vendors and agents, are typically contracted in secret, with very little transparency or understanding as to that party's role or the extent to which that entity will have access to customer's personal data. This aligns with consumer expectations and is rational.

The FCC's proposal materially advances the FCC's interests by providing a choice framework BIAS customers can actually understand and will allow those customers to make real decisions about their data.

---

[121] Tribe Comments at 27-32.
[122] Supra at pp. 21-27.
[123] FTC Comments at 24.

3. The regulation is no more extensive than necessary to serve these interests

Tribe bases his entire argument regarding this element of the *Central Hudson* test on the mere existence of a different privacy regime used by the FTC. This argument is insufficient, particularly given the serious consumer harms at issue and the FCC's proposal to address those harms. In addition, the mere existence of another privacy regime does not mean the FCC's proposal fails under the First Amendment.

As an initial matter, the D.C. Circuit has already held that "opt-out is only 'marginally less intrusive' than opt-in for First Amendment purposes."[124] So long as the FCC "carefully consider[s] the differences between [opt-in and opt-out,]" a reviewing court is likely to uphold an opt-in regime. Tribe also argues that if there is *any* alternative to a proposal that would restrict less speech, then it must do so.[125] However, as discussed above and in other comments, the opt-in regime is the correct regime when the purpose is to give BIAS customers true choice over whether their data can be used or disclosed in certain ways, instead of assuming that all customers want all of their data disclosed or sold for any purpose.

---

[124] *NCTA v. FCC*, 555 F.3d at 1002. In another case, the D.C. Circuit stated "[a]lthough the opt-in scheme may limit more Trans Union speech than would the opt-out scheme the company prefers, intermediate scrutiny does not obligate courts to invalidate a 'remedial scheme because some alternative solution is marginally less intrusive on a speaker's First Amendment interests. . . . So long as the means chosen are not substantially broader than necessary to achieve the government's interest, . . . [a] regulation [is] not . . . invalid simply because a court concludes that the government's interest could be adequately served by some less-speech-restrictive alternative.'" *Trans Union II* at 1143 (citations to *Turner Broad. System, Inc. v. FCC*, 520 U.S. 180 (1997) removed).

[125] Tribe Comments at 37.

(continued on next page)

Tribe argues that "the FTC experience demonstrates that there is nothing unique about ISPs' data collection, use, or sharing practices" and cites to the FTC's 2012 Privacy Report.[126] Tribe places too much emphasis on the FTC's findings, or lack thereof. The FCC is the agency with expertise regarding communications networks. The fact that the FTC lumps ISPs together with other "large platform providers" betrays this lack of expertise: a social network, for instance, competes with other social networks in a marketplace that runs on top of the network; in contrast, ISPs provide access to all those social networks and constitute the bottleneck through which all internet customers must pass. This distinction provides the reason for imposing neutrality obligations on BIAS providers as well as imposing a privacy regime that gives consumers real choice over data practices.

Additionally, Tribe in several places references the FTC's "successful history" of protecting privacy.[127] However, it has been under this very FTC regime that consumers have become apprehensive about their internet usage to the point of refraining from entering into commercial transactions, have come to distrust companies that collect a significant amount of data for little reason, and have come to desire more choices and transparency regarding data practices.[128] Thus, Tribe's claim that the FTC has adequately protected privacy is unpersuasive.

Last, Tribe makes several other arguments about other internet companies having access to the same data, the numerous benefits of tracking, and the need for "regulatory neutrality" across providers and technology.[129] These arguments are unavailing because they represent the mere opinion about which regime is more

---

[126] Tribe Comments at 34.
[127] Tribe Comments at 37, 35,
[128] *Supra* at pp. 21-27.
[129] Tribe Comments at 35.

appropriate, an opinion the FCC is not obligated to adhere to especially given the record evidence.

B. Notwithstanding *Sorrell*, the FCC's proposed privacy rule would not be subject to heightened First Amendment scrutiny, as some commenters have suggested

Commenters take pains to draw comparisons between the law at issue in *Sorrell v. IMS Health, Inc.* and the FCC's privacy proposal.[130] However, the two are easily distinguishable.[131] Therefore, although the Supreme Court found the government restriction on speech at issue in *Sorrell* may have gone beyond mere commercial speech regulation, the FCC's proposal clearly does not. The First Amendment standard that would likely apply to the FCC's proposed privacy rule is thus the well-established intermediate scrutiny standard for commercial speech defined in *Central Hudson*.

In *Sorrell*, the Supreme Court struck down a Vermont law on First Amendment grounds. The law in question required permission from doctors before certain prescription data could be sold or used for marketing purposes. The legislative findings further stated that the goals of marketing programs were often in conflict with the goals of the state, primarily because marketing is often one-sided in favor of brand names.[132] The Court struck down the law because the law discriminated based on viewpoint and speaker, and because the state was

---

[130] Tribe Comments at 13-14; CTIA at 76-77; Verizon Comments at 36-40, 50-53.
[131] Even if it did, the FCC should not presume that a reviewing court would apply a higher level of scrutiny merely because the Supreme Court left some ambiguity in its decision.
[132] *Sorrell*, 564 U.S. at 560-61.

(continued on next page)

attempting to suppress speech with which it disagreed.[133] The Court stated the "law's express purpose and practical effect are to diminish the effectiveness of marketing by manufacturers of brand-name drugs" and specifically targeted "detailers" and their messages "for disfavored treatment."[134] The law was also under-inclusive, as "pharmacies may share prescriber-identifying information with anyone for any reason save one: ... marketing."[135] The Court specifically noted that a more comprehensive and "coherent" policy may have done better under the First Amendment, by, for example, "allowing the information's sale or disclosure in only a few narrow and well-justified circumstances."[136] The Court also pointed to the state's "contrived choice," which is "[e]ither consent, which will allow your prescriber-identifying information to be disseminated and used without constraint; or, withhold consent, which will allow your information to be used by those speakers whose message the State supports."[137]

The FCC's proposal is not similar to the invalidated Vermont law. First, the FCC is not acting nefariously to disfavor marketing discussing particular products. The FCC has no anti-message purpose here, nor does it seek to suppress BIAS provider advertising.[138] The FCC's purposes here are purely pro-consumer and,

---

[133] *Id.* at 564-66.
[134] *Id.* at 565.
[135] *Id.* at 572.
[136] *Id.* at 573.
[137] *Id.* at 574.
[138] "[T]his NPRM supports the ability of broadband networks to be able to provide personalized services, including advertising, to consumers—while reaping the financial rewards therefrom." *NPRM* at ¶ 12. Even AT&T states that the rules "would not enable consumers to see fewer ads." AT&T Comments at 53. And that's precisely the point. The FCC is not trying to suppress advertising. It is merely trying to provide consumers choices about how those advertisements are targeted.

specifically, pro-consumer choice. To the extent this proposal burdens certain "speakers," that is the job Congress has given to it, just as Congress has burdened certain classes of speakers in privacy laws in the health, financial, and educational contexts. Title II of the Communications Act, including its privacy provisions, applies to telecommunications carriers—which the D.C. Circuit has already affirmed as including BIAS providers. Moreover, the record is replete with evidence that telecommunications carriers are special and that customers deserve additional protections as against those intermediaries.[139] The FCC lacks authority over other actors in the internet ecosystem. Opponents' arguments are, yet again, attempts to cast the entire telecom regulatory regime violates the First Amendment because it applies only to telecommunications carriers.[140] That is not the case generally, and is not the case here.

Additionally, the FCC's broadband privacy proposal is not under-inclusive as was the privacy law at issue in *Sorrell*. In that case, the Vermont law required limited use of data for one purpose. In all other instances, sharing and use of the prescription data was allowed. This is not the case with the FCC proposal, which protects nearly all customer data collected by their BIAS provider against use and disclosure unless the customer opts in or, in some limited circumstances, opts out. In this respect, the FCC's proposal fits nicely with its purpose of increasing consumer choice to ensure unfettered and uninhibited internet use.

Nor can one reasonably conclude that the opt-in/opt-out regime proposed by the FCC gives customers a "contrived choice," as the court determined the law at

---

[139] OTI Comments at 41; Ohm Reply Comments at 11-12; PK Comments at 3.
[140] For why that is not the case, see generally Brief of Amicus Curiae Reed Hundt *et al.*, *U.S. Telecom Ass'n v. FCC*, D.C. Cir. Dkt. 15-1063 (filed Sept. 21, 2015), at 17-22.

(continued on next page)

issue in *Sorrell* did.[141] Because the FCC is not supporting any particular message here, there is no choice between agreeing to use of data "without restraint" and use of data "by those speakers whose message the State supports."[142] In contrast, the FCC's proposal gives BIAS customers a real choice: opt in to the use and disclosure practices of your BIAS provider and receive all the benefits of, for instance, targeted advertising, or opt out to protect the privacy of your personal information.[143]

For these reasons, *Sorrell* is easily distinguishable from the facts and proposed rule at hand, and therefore the heightened scrutiny applied in *Sorrell* does not apply here.

III. Conclusion

The FCC's proposed broadband privacy rule is well-crafted, responds appropriately to the law and to the needs and demands of consumers, and rests on solid legal footing. The Commission should not be dissuaded by those who oppose the proposal because they stand to profit from making unfettered use of broadband customers' data without first obtaining affirmative consent to do so. The proposed rule should be adopted without delay.

---

[141] *Sorrell*, 564 U.S. at 574.

[142] *Id.*

[143] The FCC proposal includes certain uses for which BIAS provides have implied consent. OTI has already argued that this aspect of the proposal does not satisfy the statute's plain language, and should require at least opt-out consent.

/s/
Laura M. Moy, Esq.

Institute for Public Representation
Georgetown Law
600 New Jersey Avenue, NW
Suite 312
Washington, DC 20001
(202) 662-9547

Counsel for New America's Open Technology Institute

/s/
Eric G. Null, Esq.

Sarah J. Morris, Esq.

New America's Open Technology Institute[144]
740 15th St, NW
Suite 900
Washington, DC 20005

Filed July 6, 2016

[144] Many thanks to OTI's summer legal intern Ryan Morrison, who provided invaluable assistance with research and citations for these comments.